Blockchain Security Alliance

BEOSIN Blockchain Security × SUSS NiFT Node for Inclusive Fintech × LegalDAO × Footprint Analytics

Q1 2023 GLOBAL WEB3 SECURITY REPORT

& Crypto Regulatory Landscape

SECURING BLOCKCHAIN ECOSYSTEM

CONTENTS

I.
Q1 2023 Global Web3 Security Statistics

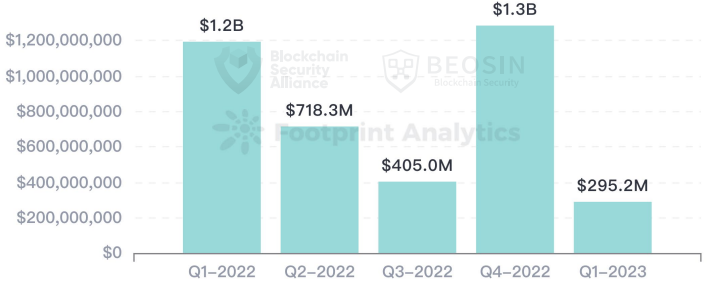
Contributors: Beosin research team —— Mario & Donny

Data source:
https://www.footprint.network/@Beosin/Footprint-Beosin-2023-Q1-Report

1. Q1 2023 Web3 Security Overview

In Q1 2023, Beosin EagleEye monitored a total of 61 major attacks in the Web3 space, with a total loss of approximately $295 million, a 77% decrease from Q4 2022. Total losses from attacks in Q1 2023 were lower than any quarter of 2022.

In addition to attacks, Beosin EagleEye also monitored 41 major rug pull incidents throughout Q1 2023, which involved a sum of approximately $20.34 million.



2022 – Q1 2023 Loss by Quarter

March saw the highest frequency of attacks, with total losses reaching $235 million, accounting for 79.7% of the overall losses in Q1.

In terms of project types, DeFi was the type with the most attacks and highest loss this quarter. A total of $248 million was lost in 42 DeFi security incidents, representing 84% of the total amount lost.

In terms of blockchain types, Ethereum accounted for 80.8% of the total losses, making it the most affected blockchain by loss amount.

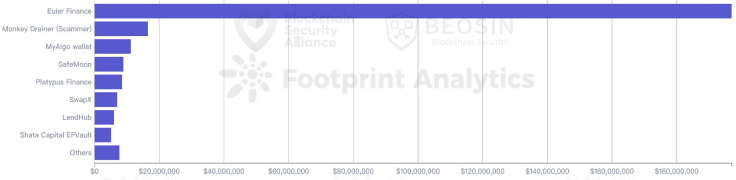
In terms of attack types, flashloans caused the most losses this quarter, with eight flashloan attacks costing approximately $198 million; the most common attack type was contract vulnerability exploits, with 27 exploits accounting for 44% of all incidents.

Approximately $200 million of stolen assets were recovered during the quarter, surpassing the recovery rate of any quarter in 2022.

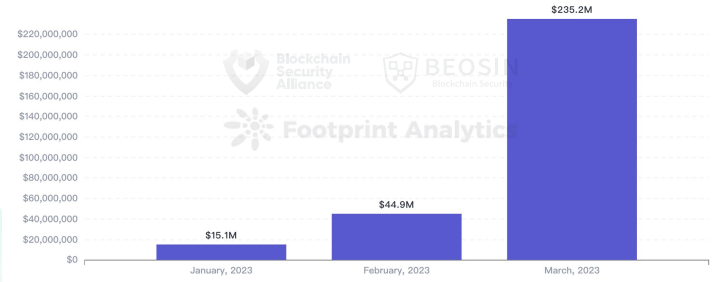
Regarding audit status, only 41% of the attacked projects had undergone an audit prior to the incidents.

2. Overview of Exploits

In the first quarter of 2023, Beosin EagleEye –– the security risk monitoring, alerting, and blocking platform monitored 61 major attacks in the Web3 space, with a total loss of approximately $295 million. There was one security incident with a loss exceeding $100 million (Euler Finance's $197 million attack). There were two incidents with losses ranging from $10 million to $100 million, and 17 incidents with losses ranging from $1 million to $10 million.



Top 10 Loss Projects 2023 Q1



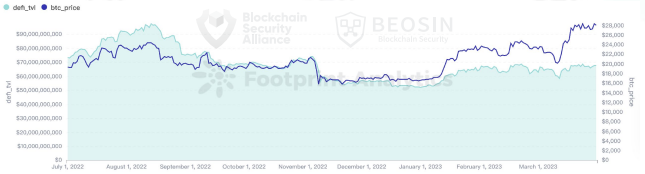
Q1 2023 Loss by Month

Overall, the total loss from attacks showed a monthly increase in the first quarter. March was a month with a high frequency of attack incidents, with total losses reaching $235 million, accounting for 79.7% of the total losses in the first quarter.

3. Types of Attacked Projects

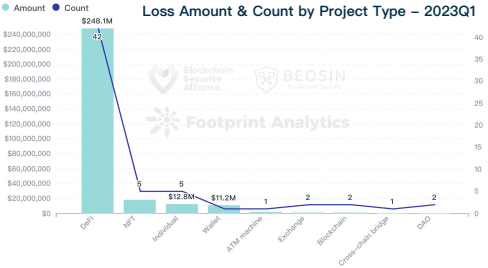
84% of loss amount was from DeFi

As the crypto market faced an extended downturn and numerous black swan events causing deleveraging, it eventually reached a bottom and began to bounce back. Concurrently, DeFi's Total Value Locked (TVL) experienced fluctuations, ultimately showing signs of recovery throughout the first quarter in tandem with cryptocurrency prices.



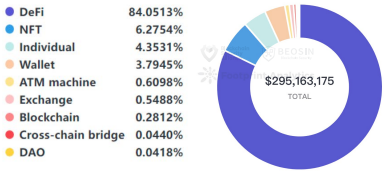
DeFi TVL & BTC PriceTrend

In the first quarter of 2023, DeFi projects experienced 42 security incidents, representing 68.9% of all events. Total DeFi losses reached $248 million, accounting for 84% of total losses. **DeFi was the project type with the most attacks and highest loss this quarter.**



NFT-related losses ranked second, totaling $18.52 million, primarily stemming from NFT phishing incidents. The third-ranked category was individual users, all of whom were victims of phishing attacks. Wallet attacks ranked fourth in terms of losses. Notably, the categories ranked 2nd to 4th in losses were all closely related to user security.

In Q1 2023, there was only one cross-chain bridge security incident, resulting in a loss of $130,000. In contrast, in 2022, 12 cross-chain bridge security incidents caused a combined loss of approximately $1.89 billion, ranking first among all project types in losses. Following the high frequency of cross-chain bridge security incidents in 2022, the security of cross-chain bridge projects significantly improved during this quarter.

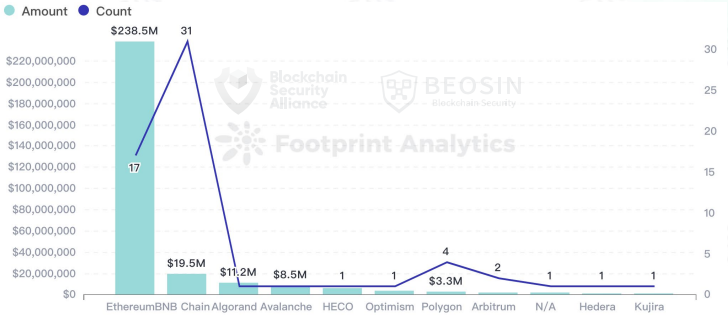


Percentage of Loss Amount by Project Type

4. Loss Amount by Chain

Ethereum account for 80.8% of losses

In Q1 2023, there were 17 major attacks on Ethereum, resulting in total losses of approximately $238 million. Ethereum saw the highest loss of any blockchain, accounting for 80.8% of the total loss.

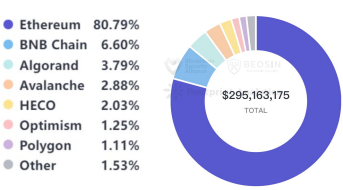


Loss Amount & Count by Chain – 2023Q1

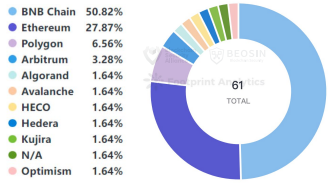
BNB Chain saw the highest number of attacks, totaling 31. Its overall losses amounted to $19.48 million, ranking second among all blockchains.

Algorand ranked third in terms of losses, primarily due to the MyAlgo wallet incident. Notably, there were no major security incidents on Algorand in 2022.

It is worth mentioning that in 2022, Solana ranked third among all blockchains in terms of losses. However, no major security incidents were detected on Solana during this quarter.

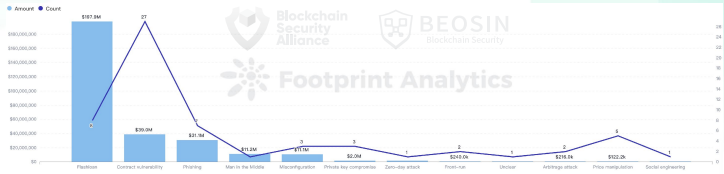


Percentage of Loss Amount by Chain



Percentage of Incident Count by Chain

5. Attack Type

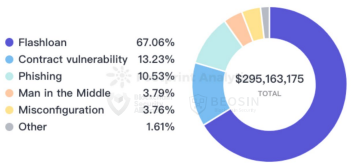


Loss Amount & Count by Attack Type – 2023Q1

Flash loans were the most common type of attack during the quarter, with eight flash loan incidents costing approximately $198 million, or 67 percent of all losses.

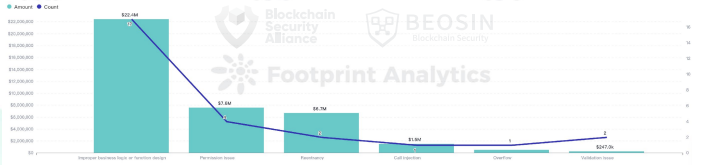
The most frequent attack type was contract vulnerability exploits, with 27 exploits accounting for 44% of all incidents. Contract vulnerabilities resulted in an accumulated loss of $39.05 million, the second highest amount of losses for all attack types.

Throughout the quarter, DeFi projects faced 42 separate attacks, with more than half (22 incidents) stemming from contract vulnerability exploits. This highlights the urgent need for DeFi projects to enhance the security of their smart contracts to avert potential threats.

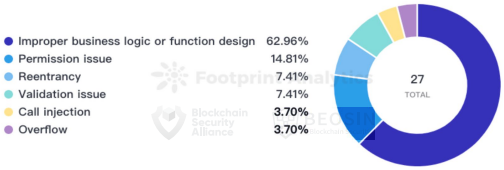


Percentage of Loss Amount by Attack Type

By type of vulnerability, the top three that caused the highest losses were improper business logic/function design, permission issues and reentrancy. A total loss of $22.44 million was lost in 17 improper business logic/function design vulnerabilities.



Loss Amount & Count by Vulnerabilities – 2023Q1



Percentage of Incident Counts by Vulnerabilities

6. Typical Security Incidents in Q1 2023

6.1 Euler Finance

Overview

On March 13th, the Ethereum-based lending project Euler Finance fell victim to a flash loan attack, resulting in a loss of $197 million.

On March 16th, Euler offered a $1 million reward for information that could help in the arrest of the hackers and the return of the stolen funds.

On March 17th, Euler Labs CEO Michael Bentley tweeted that "Euler has always been a security-conscious project". Between May 2021 and September 2022, Euler Finance underwent ten audits conducted by six blockchain security firms, including Halborn, Solidified, ZK Labs, Certora, Sherlock, and Omnisica.

Starting from March 18th until April 4th, the attacker began returning the stolen funds in installments. During this time, the attacker apologized through on-chain messages, admitting to having "messed with others' money, others' work, others' lives" and asking for forgiveness.

Txn Type: **2 (EIP-1559)** Nonce: **60** Position In Block: **12**

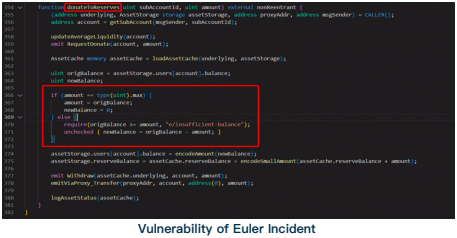
```
Jacob here. I don't think what I say will help me in any way but I still want to say it. I fucked up. I
didn't want to, but I messed with others' money, others' jobs, others' lives. I really fucked up. I'm sorry.
I didn't mean all that. I really didn't fucking mean all that. Forgive me.
```

On-chain Message from Euler Hacker

On April 4th, Euler Labs announced on Twitter that, after successful negotiations, the attacker had returned all the stolen funds.

Vulerability Analysis

In this attack, the donateToReserves function of the Etoken contract failed to properly verify the actual amount of tokens held by the user and the health status of the user's ledger after the donation. The attacker exploited this vulnerability by donating 100 million eDAI while actually having only deposited 30 million DAI.



```
function donateToReserves(uint subAccountId, uint amount) external nonReentrant {
    (address underlying, AssetStorage storage assetStorage, address proxyAddr, address msgSender) = CALLER();
    address account = getSubAccount(msgSender, subAccountId);

    updateAverageLiquidity(account);
    emit RequestDonate(account, amount);

    AssetCache memory assetCache = loadAssetCache(underlying, assetStorage);

    uint origBalance = assetStorage.users[account].balance;
    uint newBalance;

    if (amount == type(uint).max) {
        amount = origBalance;
        newBalance = 0;
    } else {
        require(origBalance >= amount, "e/insufficient-balance");
        unchecked { newBalance = origBalance - amount; }
    }

    assetStorage.users[account].balance = encodeAmount(newBalance);
    assetStorage.reserveBalance = assetCache.reserveBalance = encodeSmallAmount(assetCache.reserveBalance + amount);

    emit Withdraw(assetCache.underlying, account, amount);
    emitViaProxy_Transfer(proxyAddr, account, address(0), amount);

    logAssetStatus(assetCache);
}
}
```

Vulnerability of Euler Incident

As a result of the donation, the health status of the user's ledger met the liquidation criteria, triggering the liquidation of the lending contract. During the liquidation process, eDAI and dDAI were transferred to the liquidation contract. However, due to the large amount of bad debt, the liquidation contract applied the maximum discount for liquidation. After the liquidation was complete, the liquidation contract held 310.93 million eDAI and 259.31 million dDAI.

At this point, the health status of the user's ledger was restored, and the user could withdraw funds. The amount that could be withdrawn was the difference between eDAI and dDAI. However, there were only 38.9 million DAI actually available in the pool, so users could only withdraw this portion of the funds.

6.2 BonqDAO

Overview

On February 1st, DeFi protocol BonqDAO fell victim to a price manipulation attack. The attacker minted 100 million BEURs and then swapped for other tokens on Uniswap. The ALBT price dropped to almost zero, which further triggered the liquidation of ALBT vaults. Based on the token prices at the time of the attack, the loss was as high as $88 million. However, due to drained liquidity, the actual loss was around $1.85 million.

Vulerability Analysis

In this attack, the attacker carried out two types of attacks: **one involving borrowing a large number of tokens by manipulating prices, and the other involving profiting by manipulating prices to liquidate others' assets.**

The BonqDAO platform's oracle used the 'getCurrentValue' function instead of 'getDataBefore'. The hacker became a price reporter by staking 10 TRB tokens (worth only about $175) and manipulated the price of the WALBT token in the oracle by calling the submitValue function. After setting the price, the attacker called the createTrove function in the Bonq contract, created a trove contract, and deposited 0.1 WALBT for borrowing. Normally, the borrowing limit should be less than the price of 0.1 WALBT, ensuring that the stake ratio remains within a safe range. However, in this borrowing process, the collateral value was calculated using the TellorFlex contract. In the previous step, the attacker had already set an exceptionally high price for WALBT, resulting in the attacker borrowing 100 million BEUR tokens in this transaction.

In the second transaction, the attacker set the WALBT price exceptionally low, allowing them to liquidate the WALBT tokens staked by other users at a minimal cost.

6.3 Platypus Finance

Overview

On February 17th, Platypus Finance on Avalanche was exploited due to a checking mechanism flaw, resulting in a loss of approximately $8.5 million. However, the attacker did not implement a withdrawal function in the contract, leaving the attack proceeds stuck within the attack contract and unable to be withdrawn.

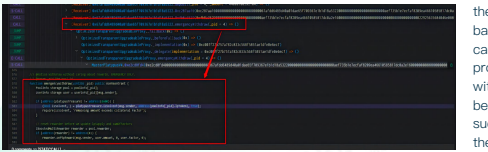
On February 23rd, Platypus announced that they had contacted Binance and confirmed the hacker's identity. Platypus also stated that they would repay at least 63% of the funds to users.

On February 26th, the French National Police arrested and summoned two suspects believed to have attacked Platypus.

Vulerability Analysis

The cause of the attack was a flaw in the checking mechanism of the emergencyWithdraw function in the MasterPlaty–pusV4 contract. It only checked whether the user's borrowing amount exceeded their borrowLimitUSP (borrowing limit) but did not verify whether the user had repaid their debt.

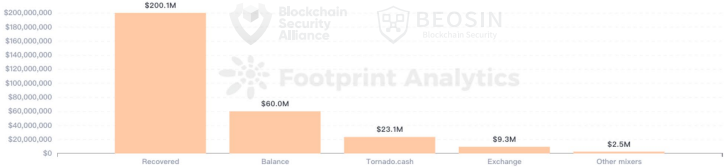
The attacker first used the AAVE contract to flashloan 44 million USDC and deposited it into the Pool contract, then minted 44 million LP–USDC. Next, the attacker called the borrow function to borrow 41.79 million USP and immediately called the EmergencyWithdraw function afterward.



Within the EmergencyWithdraw function, there is an isSolvent function to check if the balance exceeds the maximum amount that can be borrowed. If it returns true, it proceeds with the transfer operation without considering whether the debt has been repaid. Thus, the attacker was able to successfully call the function and withdraw the previously deposited 44 million LP–USDC without repaying the debt.

7. Stolen Fund Flow

In the first quarter of 2023, approximately $200,146,821 of assets were recovered, accounting for 67.8% of all stolen assets. Among them, the $197 million assets stolen from Euler Finance have been fully returned by the hacker. More examples of recovered assets include: on February 13th, the hacker who attacked dForce returned all of the stolen $3.65 million; on March 7th, the whitehat hacker who attacked Tender.fi returned the stolen funds and received a bounty of 62 ETH. **The stolen asset recovery situation in this quarter is better than any quarter in 2022.**



Stolen Fund Flow Q1 2023

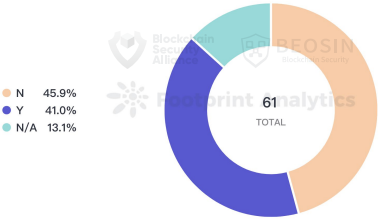
Beosin KYT AML platform found that approximately $23.13 million (7.8%) of assets were transferred into Tornado Cash, and an additional $2.54 million in assets were transferred into other mixers. Compared to last year, the proportion of stolen funds transferred into mixers this quarter has significantly decreased. In fact, since Tornado Cash faced sanctions last August, the proportion of stolen funds transferred into Tornado Cash has been on a continuous decline since Q3 2022.

At the same time, Beosin KYT AML platform discovered that about $60.02 million (20.3%) of assets are still held at hackers' addresses. Additionally, approximately $9.32 million (3.1%) of stolen assets have been transferred to various exchanges. Most of the incidents involving transfers to exchanges are low-value attacks, with a few being phishing incidents that only gained public attention days later. Due to low or delayed attention, hackers have the opportunity to transfer stolen funds into exchanges.

8. Audit Analysis

In the first quarter of 2023, among the projects that were attacked, excluding 8 incidents that cannot be measured by audits (such as phishing attacks on individual users), there were 28 projects that had undergone audits and 25 that had not.

There were a total of 27 contract vulnerability exploits this quarter, with 15 audited projects (with losses of $31.19 million) and 12 unaudited projects (with losses of $7.86 million). The overall quality of audits in the Web3 market is still not optimistic. **It is recommended that projects carefully compare auditors before choosing one, as selecting a professional auditor can effectively ensure the project's security.**

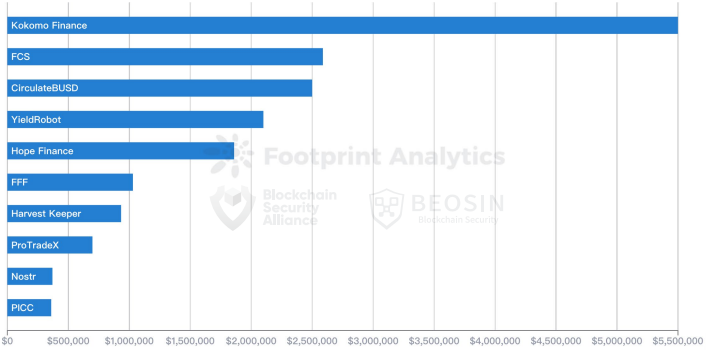


Audit Count of Attacked Projects – Q1 2023

9. Rug Pulls

In the first quarter of 2023, a total of 41 major Rug Pulls were monitored in the Web3 sector, involving approximately $20.34 million.

In terms of amount, 6 projects (14.6%) rugged with over $1 million, 12 rug pulls (29.2%) ranged from $100,000 to $1 million, and 23 rug pulls (56%) involved amounts less than $100,000.



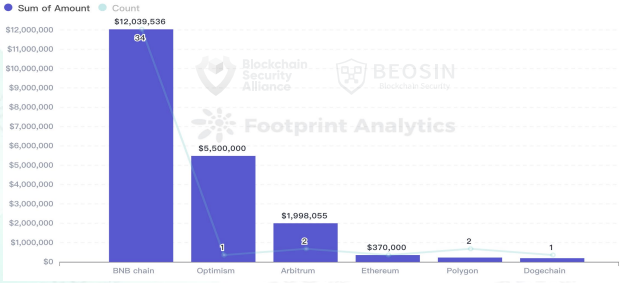
Top 10 Rug Pulls – Q1 2023

Out of the 41 Rug Pull incidents, 34 projects (83%) were deployed on BNB Chain. Why do so many scam projects choose BNB Chain? There might be several reasons:

1)BNB Chain has lower GAS fees and shorter block time intervals.

2) BNB Chain has a larger number of active users. Scam projects tend to choose chains with more active users.

3)For BNB Chain users, it is more convenient and faster to deposit and withdraw funds through Binance.



Rug Pulls by Chain – Q1 2023

10. Summary

Overall, the total losses from attacks in Q1 2023 are lower than any quarter in 2022, and the fund recovery situation is better than all quarters in 2022. After the rampant hacking in 2022, the overall security of Web3 has significantly improved in this quarter.

By project type, DeFi saw the highest frequency of attacks and the most significant losses in this quarter. There were a total of 42 security incidents in the DeFi sector, with 22 of them stemming from contract vulnerability exploitation (11 audited and 11 unaudited projects). If audited by professional security companies, most vulnerabilities can be detected and fixed during the audit stage.

User security is also a key focus this quarter. With Blur leading the NFT market back to prominence this quarter, NFT phishing incidents have also increased significantly. Carefully check whether each link is official, examine the content of signatures, verify the correctness of an address when transfer, download apps from official app stores, and install anti-phishing extensions — vigilance must be maintained at every step.

Rug Pulls continue to occur frequently this quarter, with 56% of the exit scams involving amounts less than $100,000. These projects typically have insufficient information on official websites, Twitter, Telegram, and Github, lack roadmaps or whitepapers, exhibit questionable team member information, and have a project launch-to-exit timeline not exceeding three months. It is advised that users conduct extensive background research on projects to avoid financial losses.

II.
Q1 2023 Global Crypto Regulations

Contributor: Legal Dao –– Will Liao & Joseph

Up to now, a global unified regulatory framework for Web3 and virtual assets has not been developed yet. For example, Hong Kong will introduce a regulatory framework for virtual assets in the middle of this year and the European Union is expected to introduce regulations (MiCA) aimed at unifying the European virtual asset market in the first quarter of 2024. The United Arab Emirates (Dubai) is also further developing virtual asset legislation to drive the industry's development. In the United States, the Securities and Exchange Commission (SEC) is promoting the regulation of the market through "enforcement regulation." As the United States is a global leader in the crypto industry, in addition to paying attention to the relevant virtual asset regulations and laws promulgated by countries around the world, it is also necessary to pay special attention to the relevant judicial decisions of the United States courts, as well as the regulatory enforcement of regulatory authorities.

A summary of key policies and events in the global virtual asset industry in the first quarter of 2023 is as follows:

1. Coinbase was fined $50 million by New York Department of Financial Services for violating the state's anti-money laundering laws

On January 4th, 2023, Coinbase agreed to pay a $50 million fine to the New York State Department of Financial Services (NYDFS) for allowing customers open accounts without conducting sufficient background checks.[1] Coinbase violated the New York Banking Law and the New York State Department of Financial Services' (DFS) virtual currency, money transmitter, transaction monitoring, and cybersecurity regulations. These failures made the Coinbase platform vulnerable to serious criminal conduct, including possible money laundering, suspected child sexual abuse material-related activity, and potential narcotics trafficking.

Additionally, NYDFS required Coinbase to invest $50 million to strengthen its compliance program. [2] Coinbase's Chief Legal Officer Paul Grewal said, "Coinbase and NYDFS have reached a settlement. Coinbase has taken substantial measures to address these historical shortcomings, and continues to be committed to being a leader in the virtual asset industry, including collaborating with regulators in compliance."

2. SEC charges Gemini and Genesis for the unregistered offer and sale of crypto asset securities to retail investors

On Jan. 12, 2023, SEC charged Genesis Global Capital, LLC and Gemini Trust Company, LLC for the unregistered offer and sale of securities to retail investors through the Gemini Earn crypto asset lending program.[3]

According to the complaint, in December 2020, Genesis, part of a subsidiary of Digital Currency Group, entered into an agreement with Gemini to offer Gemini customers, including retail investors in the United States, an opportunity to loan their crypto assets to Genesis in exchange for Genesis' promise to pay interest. Beginning in February 2021, Genesis and Gemini began offering the Gemini Earn program to retail investors, whereby Gemini Earn investors tendered their crypto assets to Genesis, with Gemini acting as the agent to facilitate the transaction. Gemini deducted an agent fee from the returns Genesis paid to Gemini Earn investors. As alleged in the complaint, Genesis then exercised its discretion in how to use investors' crypto assets to generate revenue and pay interest to Gemini Earn investors.

In November 2022, Genesis announced that it would not allow its Gemini Earn investors to withdraw their crypto assets because Genesis lacked sufficient liquid assets. At that time, Genesis held approximately $900 million in investor assets from 340,000 Gemini Earn investors. Then, Gemini President Cameron Winklevoss pubilished an open letter[4], addressed to the board members of Genesis parent company Digital Currency Group, accusing DCG of defrauding Gemini Earn investors, misleading them regarding DCG's solvency, making them believe that DCG had injected $1.2 billion into Genesis, and accounting fraud. Winklevoss also called for the ouster of DCG CEO Barry Silbert. Barry Silbert then denied the charges.

SEC claimed that Genesis and Gemini were partners engaged in activity that constituted the offer and sale of securities without registering. Apart from the fact that Genesis was the issuer, both are liable. "The recent collapse of crypto asset lending programs and the suspension of Genesis' program underscore the critical need for platforms offering securities to retail investors to comply with the federal securities laws. As we've seen time and again, the failure to do so denies investors the basic information they need to make informed investment decisions." said Gurbir S. Grewal, Director of the SEC's Division of Enforcement.

On Jan. 13rd, 2023, Tyler Winklevoss, co-founder of Gemini, said on Twitter that he was disappointed in the SEC's action since Gemini and other creditors are working to recover funds. The SEC's action does nothing to further our efforts and help Gemini Earn investors get their assets back. Tyler Winklevoss also pointed that Gemini Earn was regulated by NYDFS and had been in discussions with the SEC about the Earn program for more than 17 months. The SEC never raised the prospect of any enforcement action after Genesis paused withdrawals on Nov. 16th, 2022.

3. Emerging Technologies and Crypto-Assets on the list of SEC's 2023 Priorities

After the collapse of FTX and many other virtual asset platforms, SEC was criticized by the crypto market and Congress members for failing to regulate this industry in a timely manner. On Feb. 7th, 2023, the SEC's Division of Examinations announced its 2023 examination priorities including Emerging Technologies and Crypto-Assets.[5] The division publishes its examination priorities every year to provide insights into its risk-based approach, including the areas it believes present potential risks to investors and the integrity of the U.S. capital markets.

After announcing its priorities, the SEC quickly launched a new round of regulation by enforcement in the virtual asset industry, which is stricter and tougher. Kraken and its ETH staking product were the first to be targeted.

4. SEC charges Kraken with offering and selling securities through its staking services

On Feb. 9th, 2023, the SEC announced that Kraken, a San Francisco-based virtual asset exchange, agreed to pay $30 million and immediately cease offering its crypto asset Staking as a Service(SaaS) product to American users to settle the SEC's charges of failing to register the offer and sale of securities.[6] The SEC claimed that when investors provide tokens to staking-as-a-service providers, they lose control of those tokens and take on risks associated with those platforms, with very little protection. When Kraken obtains the key of investors' assets, it can control their assets and use them for any purpose without the disclosures that investors deserve and promises that investors can have high investment returns.

Gary Gensler, chair of the SEC, personally appeared on the scene and explained in a video why Kraken SaaS product needs to comply with the US Securities Law: "When a company or platform provides you with these types of products and promises returns, no matter what they call their services, whether it is lending, earn rewards, APY or staking, this kind of behavior of providing investment contracts in exchange for investor funds should be protected by the federal securities laws...This enforcement action should clearly indicate to the market that SaaS product providers must register and provide comprehensive, fair and real information disclosures and investor protection."

The determination of securities for Kraken's SaaS product has caused great panic in the crypto market, but in fact, the difference between the SaaS product of Kraken and ETH Staking(Solo Staking) are significant. From the SEC's announcement, it can be roughly seen how the SEC determined that Kraken's SaaS product was a security. Firstly, Kraken receives investor funds (totally control), and secondly the funds were mixed with a fund pool and used by Kraken for any purposes (what the funds are used for is unknown). Thirdly, Kraken actually promised a maximum return of 21% (the return for ETH Staking on the Ethereum Foundation's website is 3%-5%). Finally, investors only participated in investment through Kraken's efforts to achieve the return. This meets all the criteria of the Howey test, which constitutes an "investment contract" and is a type of securities transaction.

5. NYDFS instructed Paxos to cease issuing BUSD stablecoin

On Feb. 13th, 2023, Binance CZ stated that NYDFS instructed Paxos to cease issuing new BUSD stablecoin(BUSD is a stablecoin wholly owned and managed by Paxos). At the same time, Paxos confirmed that it received a notification of potential charges in connection with its BUSD product from the SEC.

Paxos is a New York–based tablecoin issuer and operates under a BitLicense from the NYDFS. It is regulated by the state's Department of Financial Services (NYDFS). The minted BUSD stablecoins are on Ethereum and backed 1:1 with US dollar–denominated reserves according to the requirement of Guidance on the Issuance of U.S. Dollar–Backed Stablecoins[7] published by NYDFS in June, 2022. NYDFS has the right to ask Paxos to stop issuing BUSD or directly stop Paxos' Bitlicense license on the grounds that it has not completed the user's regular risk assessment and due diligence commitments to prevent bad behavior (such as money laundering) and other compliance matters. The NYDFS issued the order "as a result of several unresolved complicated issues related to Paxos' oversight of its relationship with Binance".

Paxos responded to NYDFS's regulatory measures through its official website, saying that effective February 21st, Paxos will cease issuance of new BUSD tokens as directed by and working in close coordination with the NYDFS and will terminate its partnership with Binance on BUSD. It will launch Pax Dollar (USDP) to replace the minted BUSD tokens.[8]

Regarding this incident, CNBC stated in a report that Paxos' BUSD product should be distinguished from Binance–Peg BUSD issued by Binance itself. Binance's self–issued BUSD, which is not directly regulated by NYDFS, is independently wrapped and issued by the crypto exchange on blockchains beyond Ethereum. In other words, Binance can take a single Paxos–issued BUSD, create an analogous BUSD on another blockchain (like Binance's own blockchain) and freeze a corresponding Paxos–issued BUSD.[9] NYDFS stated: "The department has not authorized Binance–Peg BUSD on any blockchain, and Binance–Peg BUSD is not issued by Paxos."

On February 13th, 2023, Paxos announced that it had received a Wells notice from the SEC on February 3rd. The Wells notice stated that the staff of the SEC was considering recommending an action alleging that BUSD is a security and that Paxos should have registered the offering of BUSD under the federal securities laws. The SEC's Wells Notice is a formal notice telling the recipient that the regulator plans to take relevant enforcement actions against it, and the recipient has the opportunity file a written non–prosecution statement with the SEC. Paxos stated that Paxos categorically disagrees with the SEC staff. Paxos has always prioritized the safety of its customers' assets. BUSD issued by Paxos is always backed 1:1 with US dollar–denominated reservesfully segregated and held in bankruptcy remote accounts. We will engage with the SEC staff on this issue and are prepared to vigorously litigate if necessary.[10]

There are many speculations about the reasons for the SEC's regulatory actions. One view is that, combined with Kraken's pledged interest–earning product being fined by the SEC, it is speculated that the US SEC's crackdown on BUSD may be related to its deposit and interest–earning products. Stablecoins may be considered as money market mutual funds (MMMF), even though they have no expectation of profit. MMMF is a security offered by a company that invests in assets such as commercial paper, certificates of deposit, and treasury bonds. It is regulated by the SEC, and Circle has a similar product, so it may also be subject to similar regulation.

Subsequently, the NYDFS explained more problems in a report with Bloomberg[11]. The reason for the NYDFS to order Paxos to stop issuing BUSD does not appear to have anything to do with the possibility of considering stablecoins as securities, and the real reason may have to do with Circle's complaint that Binance–Peg BUSD's reserves were mismanaged.

6. SEC's new regulations for virtual asset custody (Proposal)

On February 15th, 2023, the SEC released a draft proposal on qualified custodians for investment advisors[12], which further enhanced the custody requirements for virtual assets and extended the requirements to investment advisors such as funds, requiring them to use qualified custodians. Qualified Custodians hold related virtual assets. This proposal aims to increase the threshold for investment consultants to improperly use and abuse user assets, and may further squeeze the living space of small and medium-sized virtual asset platforms.

SEC Chairman Gary Gensler specifically emphasized that the current regulations (the 2009 regulations) can cover a large number of virtual assets and make them regulated. Although some virtual asset trading and lending platforms claim to be able to take custody of investors' virtual assets, this does not mean that they are qualified custodians. As a result, in the event of a "bank run" and other similar situations, the assets of investors become the assets of failed companies, which seriously violates the interests of investors. Both investors and investment advisers will be afforded the protections they deserve through this expanded Qualified Custodian Regulation for Investment Advisers. [13]

It can be seen that after the collapse of FTX, the SEC put forward higher requirements for the custody business of the virtual asset platform. The SEC's proposal will encourage investors to entrust their virtual assets with institutions or mainstream banks with custody licenses. At the same time, this will give banking financial regulators the ability to scrutinize virtual asset activities.

In practice, we have seen that entities with custody business have obtained relevant trust licenses (Trust Charter) at least at the state level, and are subject to the supervision of state financial regulatory agencies. Anchorage Digital Bank has further obtained approval from the Office of the Comptroller of the Currency (OCC), which is in charge of U.S. banking institutions, at the federal level, becoming a truly federally chartered virtual asset bank. [14]

7. SEC Charges Terraform and CEO Do Kwon with orchestrating a multi-billion dollar crypto asset securities fraud

On February 16th, 2023, the SEC issued an announcement announcing a civil lawsuit against Terraform Labs, the Singapore company behind the TerraUSD stablecoin, and its CEO Do Kwon, alleging that it failed to disclose information about the virtual asset securities to the public as required, And misled investors through false descriptions before the crash.[15] Do Kwon's behavior may constitute virtual asset securities fraud, which violates the US Securities Act and Securities Exchange Act on the issuance and sale of unregistered securities, anti-fraud and other laws and regulations. Notably, the SEC explicitly charges in the filing that Luna and UST are unregistered securities.

The SEC's complaint alleges that Terraform and Do Kwon marketed virtual asset securities to investors seeking profit, repeatedly claiming that the tokens would increase in value. For example, they touted UST as a "yielding" stablecoin that pays up to 20% interest through the protocol. The SEC also alleges that, in marketing LUNA tokens, Terraform and Kwon repeatedly misled and deceived investors into believing that a popular South Korean mobile payment app added value to LUNA by using the Terra blockchain to settle transactions. At the same time, Terraform and Kwon are also alleged to have misled investors about the stability of UST. In May 2022, UST was de-pegged from the US dollar, and LUNA tokens plummeted to almost zero.

It is reported that Do Kwon was arrested in Montenegro on March 23rd, 2023. Montenegro Interior Minister Filip Adzic said via Twitter that the police detained Kwon, a South Korean citizen suspected of being one of the most wanted persons, at Podgorica airport for forging documents while he was trying to fly to Dubai using false documents. After his identity was confirmed, the United States and South Korea successively filed requests for Do Kwon's extradition.

8. Utah State Legislature passes Utah DAO Act

On March 1st, 2023, The Utah State Legislature passed Act HB 357, the Utah Decentralized Autonomous Organizations Act (Utah DAO Act)[16]. It means that DAO, as an organization form, has legal recognition in the US again after Wyoming DAO Supplement. The act will go into effect on January 1st, 2024.

The Utah DAO Act gave the DAO an independent, new legally recognized organizational form. In terms of legal nature, DAO has a legal personality that is independent and different from other members, can sue and respond to lawsuits in the name of its own DAO, and has the right to conduct any legal affairs. In this regard, the Utah DAO Act is different from Wyoming's regulatory framework that only incorporates DAO into a Limited Liability Company (LLC), but instead creates a new legal entity for DAO LLD, which is clearly distinguished from LLC.

In terms of limitation of liability, the system of limited liability applies. Take all the assets of DAO as the upper limit of liability, and assume limited liability to the outside world; after the assets of DAO are exhausted, DAO members will not be liable; as DAO members, they will not take personal responsibility for the mistakes or negligence of other DAO members, only as DAO members Take responsibility for the on-chain contributions promised by the DAO. In this regard, the problem that the U.S. Commodity Trading Commission (CFTC) required Ooki DAO members to assume the unlimited joint and several liability of DAO with their personal assets was solved in court.

The Utah DAO Act also regulates the taxation system of DAO (the default is in the form of partnership, which can be changed to the form of a company), the legal representative (to facilitate the handling of affairs that cannot be completed on the chain, and does not bear joint and several liabilities), DAO members and governance (token holding The identification of human beings) and other aspects have been innovatively stipulated, aiming at the organic integration between the DAO on the chain and the legal entity off the chain.

9. Crypto-friendly banks Silvergate Bank & Signature Bank were taken over by the FDIC

On March 1st, 2023, Silvergate Bank announced that it was unable to submit the annual 10-K report to the SEC on time, and that it may face the dilemma of "insufficient capital". [17] Subsequently, a number of partners including Coinbase, Circle, Tether, and Galaxy Digital have distanced themselves from it, causing Silvergate Bank's stock price to plummet.

Silvergate Bank, a community retail bank based in California, positions itself as a gateway to the virtual asset industry, accepts deposits from virtual asset exchanges and institutions, and has established its own virtual currency settlement payment network – "Silvergate Exchange Network" (SEN) Real-time payment system. The system enables virtual asset exchanges, institutions and customers to exchange virtual currencies for fiat currencies. With the development of the virtual asset industry, Silvergate Bank landed on the New York Stock Exchange in November 2019 with a share price of $13.

With virtual asset prices falling and many virtual asset exchanges and lending institutions collapsing in late 2022, concerns arose about the potential impact of deposit losses and credit exposure on Silvergate Bank, and on the broader virtual asset industry potential impact. FTX crashes in November 2022, resulting in Silvergate Bank having over $1 billion in exposure to FTX. What's more serious is that the collapse of FTX caused a serious "bank run". Silvergate Bank processed more than $8.1 billion in withdrawals. In order to meet the large number of withdrawals, Silvergate Bank was forced to suffer huge discount losses and urgently sold about $5.2 billion assets, and received a $4.3 billion loan from the Federal Home Loan Bank. According to Silvergate Bank's financial report for the fourth quarter of 2022, its customer deposits under management plummeted to $3.8 billion, far below the $11.9 billion in the third quarter, and it incurred a loss of nearly $1 billion.

On March 8th, 2023, Silvergate Bank stated in a filing with the SEC that it will wind up operations and voluntarily liquidate Silvergate Bank in accordance with applicable regulatory procedures. [18] "The bank's liquidation plan included full repayment of all deposits and consideration of how best to resolve claims and preserve the residual value of its assets, including its know-how and tax assets." Subsequently, Silvergate Bank was federally insured Corporation (FDIC) takes over.

On March 10th, 2023, a brief 48-hour bank run against the backdrop of a Federal Reserve rate hike resulted in a severe collapse at Silicon Valley Bank (SVB) (the 16th largest bank in the U.S. with a 40-year history). Liquidity issues, and was taken over by the FDIC. It was the second-largest bank failure in U.S. history after Washington Mutual collapsed in 2008. On March 12th, 2023, the Treasury Department, the Federal Reserve and the FDIC issued a joint statement, stating that after consultations, they agreed to complete the rescue of Silicon Valley Bank through the FDIC in a manner that fully protects all depositors. Starting from Monday, March 13, depositors will Can use, get all their money back, and the losses associated with the SVB resolution will not be borne by the taxpayers. [19]

Due to the influence of Silicon Valley Bank, on March 12th, 2023, the U.S. Department of the Treasury, the U.S. Federal Reserve and the FDIC issued a joint statement announcing the closure of the encryption-friendly bank Signature Bank on the grounds of "systemic risk" to prevent the banking crisis from continuing to spread [20] At the same time, NYDFS appointed FDIC as receiver for the disposed assets, even though Signature Bank had recovered from the impact of Silicon Valley Bank at that time and held a good balance sheet.

U.S. banking regulators (the OCC at the federal level and the state financial regulators at the state level, such as NYDFS) have the right to revoke their business licenses due to poor management or insolvency of their subsidiaries. When a bank ceases to operate, the Federal Deposit Insurance Corporation (FDIC) is appointed as the manager or receiver of the troubled bank (which plays an integral role in the rescue or liquidation of the bank), protecting depositors' deposits and minimize the negative impact of bank closures on the overall financial system.

The closure of Silvergate Bank and Signature Bank, two crypto-friendly banks, has brought the virtual asset industry back to the days when virtual assets had no formal bank accounts many years ago, because any newly established company has no chance of obtaining a banking license immediately.

10. SEC charges Justin Sun with selling unregistered securities, alleged Fraud and market manipulation

On March 22nd, 2023, the SEC issued an announcement announcing the prosecution of Justin Sun and his three wholly-owned companies Tron Foundation Limited, BitTorrent Foundation Ltd. and Rainberry Inc. (Sun and its affiliates). [21] In the lawsuit filed by the SEC in the U.S. District Court for the Southern District of New York, Sun and its affiliates provided multiple online "bounty projects" for unregistered securities, and issued and sold TRX and BTT, which directly guided the sense of Interested parties advertise TRX and BTT on social media, join or recruit others to join Tron-affiliated Telegram and Discord channels, and create BitTorrent accounts in exchange for TRX and BTT allocations. According to the indictment, the offering and sale of these unregistered securities violated Section 5 of the Securities Act.

The SEC also accused Sun of planning a Wash Trading scheme to artificially exaggerate the trading volume of TRX in the secondary market, involving a large number of real-time buying and selling transactions, making TRX appear to be actively traded, while there is no actual change in actual beneficial ownership, which violates the Anti-fraud and market manipulation provisions of the U.S. Securities Act. From at least April 2018 to February 2019, Sun directed the team he controlled to conduct more than 600,000 fake TRX transactions between the two accounts, averaging between 4.5 million and 7.4 million per day. Sun also provided a large supply of TRX, sold TRX to secondary markets, and made $31 million in proceeds from illegal, unregistered token offerings and sales. In addition, the SEC also accused Sun of planning a plan to pay celebrities to sell TRX and BTT, and concealing from the public information about the celebrity's remuneration, creating false impressions and violating the relevant provisions of the Securities Exchange Act.

"This case again demonstrates the very high risks investors face when offering and selling virtual asset securities without proper disclosure," said SEC Chairman Gary Gensler. "As alleged, Sun and its affiliates not only Issuing and selling unregistered securities to U.S. investors, and obtaining millions of illegal proceeds at the expense of investors, and they also falsely traded on unregistered virtual asset trading platforms to create a false sense of active trading. Misleading appearances. Sun further lured investors into buying TRX and BTT by orchestrating a celebrity promotion where he and the celebrities concealed the fact that they paid for the promotion."

"While we are neutral on controversial technologies, we are by no means neutral when it comes to investor protection," said Gurbir S. Grewal, Director of the SEC Division of Enforcement. "As alleged in the complaint, Sun and its affiliates used a The age-old playbook of misleading and harming investors by first offering securities without adhering to registration and disclosure requirements and then manipulating the market for those securities. Meanwhile, Sun pays celebrities with millions of followers on social media , to promote products that are unregistered securities, while specifically instructing them not to disclose their compensation. This is exactly what the Securities Act of the United States is designed to prevent."[22]

11. The White House's Economic Report of the President brings a negative influence on the crypto industry

On March 22nd, 2023, for the first time, the Economic Report of the President[23] included a chapter on digital assets, claiming that blockchain technology improves financial innovations and drives the rise of virtual assets. However, the report listed the negative aspects of virtual assets and blasted crypto for having no use and no value. Virtual assets can not serve as a store of value and they are not effective tools for payment.

"Although advocates often claim that digital assets, particularly crypto assets, are a revolutionary innovation, the design of these assets frequently reflects an ignorance of basic economic principles that have been learned in economics and finance over centuries. This inadequate design is often detrimental to consumers and investors." Virtual assets are claimed to be investment vehicles and currency, which exists a contradiction since as a type of currency, it should be stable and has limited volatility but as a type of high risk assets, it should have high volatility to make investors achieve high returns. The higher risk an asset has, the less possibility it has to be a type of currency.

12. CFTC charges Binance and its founder CZ with willful evasion of Federal laws and operating an illegal virtual asset derivatives exchange

On March 27th, 2023, the U.S. Commodity Futures Trading Commission (CFTC) announced that it has filed a civil enforcement action in the U.S. District Court for the Northern District of Illinois charging Changpeng Zhao and three entities that operate the Binance platform with numerous violations of the Commodity Exchange Act (CEA) and CFTC regulations. At the same time, the complaint also charges Samuel Lim, Binance's former chief compliance officer, with aiding and abetting Binance's violations.[24]

According to the complaint, Binance has offered and executed commodity derivatives transactions to and for U.S. persons from July 2019 through the present. As alleged, Binance's compliance program has been ineffective and, at Zhao's direction, Binance has instructed its employees and customers to circumvent compliance controls, including through VPNs and setting up shell companies. The defendants allegedly chose to knowingly disregard applicable provisions of the CEA while engaging in a calculated strategy of regulatory arbitrage to their commercial benefit.[25]

Therefore, the CFTC accused CZ and its affiliates of violating relevant laws and regulations related to futures trading, illegal off-exchange commodity options, unregistered futures commission merchants, designated contract markets, or swap execution agencies through civil lawsuits, negligence in supervision, failure to implement KYC or anti-money laundering processes, and establishment of substandard compliance programs, etc. In its continuing litigation against the defendants, the CFTC seeks disgorgement, civil monetary penalties, permanent trading and registration bans, and a permanent injunction against further violations of the CEA and CFTC regulations, as charged.

CFTC Chairman Rostin Behnam said: "Today's enforcement action demonstrates that there is no location, or claimed lack of location, that will prevent the CFTC from protecting American investors. I have been clear that the CFTC will continue to use all of its authority to find and stop misconduct in the volatile and risky digital asset market...For years, Binance knew they were violating CFTC rules, working actively to both keep the money flowing and avoid compliance. This should be a warning to anyone in the digital asset world, there is no location, or claimed lack of location, that will prevent the CFTC from protecting American investors."

13. The regulation of virtual assets in Hong Kong is about to come into force

Since November 2022, the Hong Kong Financial Services and the Treasury Bureau (Finance Bureau) officially released the "Policy Declaration on the Development of Virtual Assets in Hong Kong", marking that Hong Kong is one of the most international and economically active financial regions in China. Officially joined the tide of competing for the world's virtual asset center. Immediately afterwards, on February 20th, 2023, the Hong Kong Securities and Futures Commission (hereinafter referred to as the "SFC"), on the basis of the previous virtual asset regulatory framework, issued the "Applicable to Virtual Asset Transactions Licensed by the Securities and Futures Commission". The Consultation Document on the Suggested Regulatory Regulations for Platform Operators (hereinafter referred to as the Consultation Document)[26] marks that Hong Kong's supervision of the Web3 virtual asset industry is about to enter the stage of implementation, and more detailed and operable regulations are coming soon.

14. The United Arab Emirates (UAE) has passed a new virtual asset law

In Jan. 2023, The United Arab Emirates (UAE) has passed a new law that governs virtual assets, setting up the country's initial regulatory regime for the cryptocurrency space at the federal level. The new law ensures that entities that engage in crypto activities must secure a license and approval from the new regulator. Failure to comply leads to heavy sanctions, such as a fine of up to 10 million AED ($2.7 million), disgorgement of profits and even criminal investigation by the public prosecutor. In March, the Central Bank of the United Arab Emirates (CBUAE) made progress toward the full launch of its CBDC, called the digital dirham. CBDC is a type of digital currency issued and backed by a central bank.

15. Japan's Finance Ministry planned to launch an expert panel for CBDC

Japan's Finance Ministry planned to establish an expert panel in April to explore the framework and technical problems, including the possible issuance of a central bank digital currency (CBDC). Japan also planned to cooperate with G7 members to address the regulation issue of crypto assets and made it as a discussion topic in the G7 Summit in May.

16. The Political Affairs Committee of South Korea's National Assembly proposed and debated the legislation Act related to virtual assets

In March 2023, The Political Affairs Committee of South Korea's National Assembly convened the first bill review branch to propose and debate virtual asset-related measures. In April, a public hearing will be conducted to hear expert viewpoints. There are currently 18 bills related to virtual assets pending at the Political Affairs Committee of the National Assembly of Korea.

17. Thailand SEC issued rules on management of digital wallets for custody of digital assets and keys

In Jan 2023, Thailand's Securities and Exchange Commission has issued regulations for crypto custody providers to establish a digital wallet–management system to ensure the safety and efficiency of customers' assets and keys custody. The regulations took effect on Jan. 16th 2023. In March, deputy government spokeswoman Rachada Dhnadirek stated that Thailand's cabinet agreed to waive corporate income tax and value–added tax for companies that issue digital tokens for investment. The tax exemption will apply to both the primary and secondary markets for firms and registered entities that issue ICO(Initial Coin Offerings) and token investors, but utility tokens will not be eligible.

18. The Bank of Israel on Wednesday published principles for regulating stablecoin activity

In Feb. 2023, Israel's Central Bank Proposes Rules for Stablecoins. The reserve assets that will be held by a stablecoin issuer must cover 100% of its liabilities to the stablecoin holders. In terms of the identity of the regulators, it is proposed that stablecoin issuers will require licensing: for a coin that does not have systemic importance, the licensing shall be by the Capital Market Authority; otherwise the licensing shall be by the Banking Supervision Department. The proposed regulation principles are open to public comment and feedback until April 15th, after which the bank will make required changes and recommend legislation to the government.

REFERENCE:

[1] NYDFS: Consent Order Issued to Coinbase, Inc.
https://www.dfs.ny.gov/system/files/documents/2023/01/ea20230104_coinbase.pdf
[2] Coinbase and NYDFS reach agreement to resolve compliance investigation
https://www.coinbase.com/blog/Coinbase-and-NYDFS-reach-agreement-to-resolve-compliance-investigation
[3] SEC Charges Genesis and Gemini for the Unregistered Offer and Sale of Crypto Asset Securities through the Gemini Earn Lending Program
SEC.gov | SEC Charges Genesis and Gemini for the Unregistered Offer and Sale of Crypto Asset Securities through the Gemini Earn Lending Program
[4] An Open Letter to the Board of Digital Currency Group
https://assets.ctfassets.net/jg6lo9a2ukvr/7wOuIDB8ZUVCqVJzocDL/394114442846c3daccc7b05978e267e0/2023-01-10_-_Gemini_-_Open_Letter_to_DCG_Board.pdf
[5] SEC Division of Examinations Announces 2023 Priorities
SEC.gov | SEC Division of Examinations Announces 2023 Priorities
[6] SEC, Kraken to Discontinue Unregistered Offer and Sale of Crypto Asset Staking–As–A–Service Program and Pay $30 Million to Settle SEC Charges
SEC.gov | Kraken to Discontinue Unregistered Offer and Sale of Crypto Asset Staking–As–A–Service Program and Pay $30 Million to Settle SEC Charges
[7] NYDFS, Guidance on the Issuance of U.S. Dollar–Backed Stablecoins
Industry Letter – June 8, 2022: Guidance on the Issuance of U.S. Dollar–Backed Stablecoins | Department of Financial Services
[8] Paxos Will Halt Minting New BUSD Tokens
Paxos Will Halt Minting New BUSD Tokens – Paxos
[9] Crypto firm Paxos to face SEC charges, ordered to stop minting Binance stablecoin
Paxos facing SEC charges, ordered to stop minting Binance stablecoin
[10] Paxos Issues Statement
Paxos Issues Statement – Paxos
[11] Bloomberg, Stablecoin Issuer Circle Warned Watchdog About Binance Token
Stablecoin Issuer Circle Warned Watchdog About Binance Token (1)
[12] SEC Proposes Enhanced Safeguarding Rule for Registered Investment Advisers
SEC.gov | SEC Proposes Enhanced Safeguarding Rule for Registered Investment Advisers
[13] Gary Gensler, Statement on Proposed Rules Regarding Investment Adviser Custody
SEC.gov | Statement on Proposed Rules Regarding Investment Adviser Custody
[14] Anchorage Trust Company Convert to a National Trust Bank
https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-6a.pdf
[15] SEC Charges Terraform and CEO Do Kwon with Defrauding Investors in Crypto Schemes
https://www.sec.gov/news/press-release/2023-32
[16] Uath, H.B. 357 Decentralized Autonomous Organizations Amendments
https://le.utah.gov/~2023/bills/static/HB0357.html
[17] Silvergate SEC Filing
https://ir.silvergate.com/sec-filings/default.aspx
[18] Silvergate, FORM 8-K, 03/08/2023
https://ir.silvergate.com/sec-filings/sec-filings-details/default.aspx?FilingId=100117321969
[19] Silicon Valley Bank, Joint Statement by Treasury, Federal Reserve, and FDIC
https://www.federalreserve.gov/newsevents/pressreleases/monetary20230312b.htm
[20] Signature Bank, Joint Statement by the Department of the Treasury, Federal Reserve, and FDIC
https://www.fdic.gov/news/press-releases/2023/pr23017.html
[21] SEC Charges Crypto Entrepreneur Justin Sun and his Companies for Fraud and Other Securities Law Violations
https://www.sec.gov/news/press-release/2023-59
[22] SEC v. Justin Sun, et al.
https://downloads.coindesk.com/legal/justin.PDF
[23] Economic Report of the President
https://www.whitehouse.gov/wp-content/uploads/2023/03/ERP-2023.pdf
[24] CFTC Charges Binance and Its Founder, Changpeng Zhao, with Willful Evasion of Federal Law and Operating an Illegal Digital Asset Derivatives Exchange
https://www.cftc.gov/PressRoom/PressReleases/8680-23
[25] Commodity Futures Trading Commission v. Zhao et al
https://www.courtlistener.com/docket/67092867/1/commodity-futures-trading-commission-v-zhao/
[26] 有關適用於獲證券及期貨事務監察委員會發牌的 虛擬資產交易平台營運者的 建議監管規定的諮詢文件
https://apps.sfc.hk/edistributionWeb/api/consultation/openFile?lang=TC&refNo=23CP1

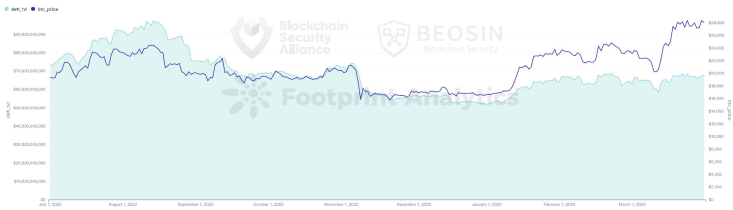
III.
DeFi Overall Trend and Major Events Recap

Contributor: SUSS NiFT -- Jesse Zheng

1. DeFi Overall Trend

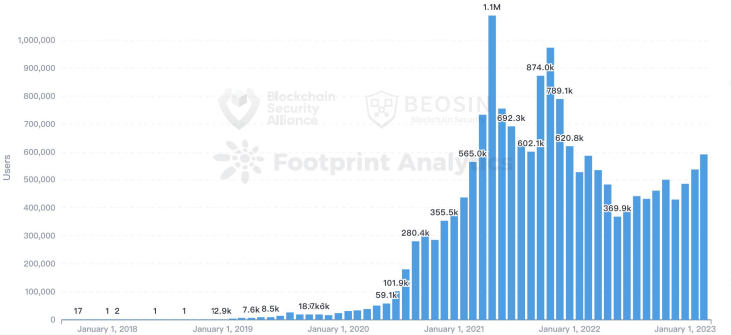
We will analyze the trends of DeFi in the first quarter by tracking the on-chain TVL, user activity, monthly protocol revenue, token performance, and capital flow of the overall DeFi ecosystem.

After a prolonged downtrend and multiple black swan events causing deleveraging, the crypto market experienced a rebound. DeFi's TVL fluctuated and recovered during Q1, growing from $52 billion to $67.7 billion as a result of price changes.



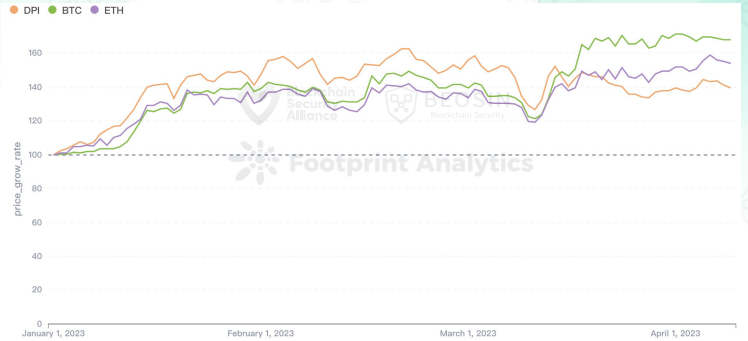
DeFi TVL & BTC Price Trend

The number of monthly unique DeFi users saw a continuous increase for four consecutive months, indicating a revival of on-chain activity.



Monthly Unique DeFi Users

While the overall fundamentals of DeFi improved, the performance of DeFi tokens in the first quarter still lagged behind that of BTC and ETH. This can be attributed to two factors: firstly, BTC and ETH typically lead the charge during the transition from bear to bull markets, and secondly, the design of most tokens failed to adequately capture the value of their respective protocols.



DPI vs BTC vs ETH Token Price

Throughout 2021 and 2022, major Ethereum competitors made significant progress, and in 2023, Ethereum Layer 2 solutions took the baton, inheriting the value overflow from Ethereum. In Q1 2022, the total value locked (TVL) in Layer 2 increased from $4.126 billion to $7 billion, while Ethereum's TVL grew from $22.5 billion to $29.68 billion during the same period. The leading Optimism Rollup project, Arbitrum, announced its token launch, marking the beginning of a new development phase.

On February 16th, zkSync entered the zkSync Era, allowing developers to engage in closed construction on the mainnet, with plans to open access to users in the next phase. Polygon scheduled the launch of the zkEVM mainnet Beta version for March 27th. Centralized exchange Coinbase also announced on February 23rd that it would build its Layer 2 network, Base, on OP Stack. It can be seen that in the future, most on-chain activities will take place on Layer 2 networks with better performance and lower costs, while Layer 1 will primarily serve as a security, consensus, and settlement layer.

2. DeFi Major Events

Ethereum Shanghai upgrade

Undoubtedly, the most significant event in the blockchain industry in 2023 is the Ethereum Shanghai upgrade. In September 2022, Ethereum underwent the Merge, transitioning from Proof of Work (PoW) to Proof of Stake (PoS) consensus mechanism. Initially planned for March, the Shanghai upgrade was ultimately confirmed for April 12th by Ethereum core developers during a conference call. One of the main focuses of this upgrade is to allow ETH stakers to withdraw their staked ETH.

Currently, only 15.35% of ETH is staked, compared to approximately 40% for other PoS projects. The primary reason for this discrepancy is the inability to withdraw staked ETH, which creates liquidity and security concerns. It is expected that, after the withdrawal functionality has been operating smoothly for some time, the demand for staking ETH will increase significantly. Liquid Staking Derivatives (LSD) protocols have already gained widespread attention in the market.

Lido is the largest LSD protocol, holding 74.64% of the market share and continuing to expand its dominance. However, this has also led to centralization concerns. At present, 31.29% of staked ETH is held within Lido.

Coinbase is the largest centralized liquidity derivative service provider, occupying 14.74% of the market share due to its brand advantage and convenience. However, its 3.78% staking yield is significantly lower than that of other decentralized service providers.

Rocket Pool is the second-largest liquid staking derivatives protocol, holding 5.62% of the market share. While it trails far behind the market leader Lido, it outperforms the fourth-ranked Frax Finance by a noticeable margin.

Frax Finance is an emerging star in the liquid staking protocol space, rapidly rising with a significantly higher annualized yield of 11.57% compared to other protocols. After staking ETH in Frax and receiving frxETH, users have two options: 1. Join the Curve frxETH-ETH liquidity pool (LP) and receive $CRV, $CVX, and $FXS rewards. 2. Stake frxETH to obtain sfrxETH, receiving basic staking rewards and the staking rewards originally belonging to the LP frxETH (frxETH in the LP is not eligible for staking rewards). This is primarily due to Frax Finance being the largest holder of CRV.

The completion of the Shanghai upgrade could potentially promote the adoption of Ethereum staking derivatives like stETH in lending protocols, establishing ETH staking rates as the on-chain benchmark interest rate. Users can further increase their yields through the leverage functions of lending protocols, which in turn may contribute to the growth of lending protocol volumes and revenues.

There are currently concerns in the market about the excessive centralization of PoS nodes. To address this issue, distributed validation node protocols like Obol Network have created distributed validation clusters, allowing different validation nodes to come together and stake as a single entity. Individual stakers can join the cluster without worrying about a single point of failure, as other nodes in the cluster will continue to operate, making this approach more resilient and dynamic than a single node. This method increases the decentralization of the Ethereum network and enhances its censorship resistance. SSV Network also offers similar services.

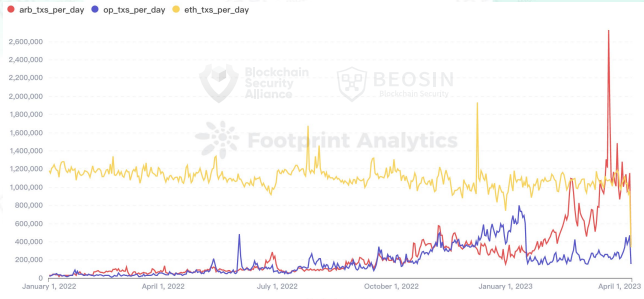
While the market is excited about the upcoming Ethereum Shanghai upgrade, it has also drawn regulatory attention. On February 9th, the US Securities and Exchange Commission announced that the Kraken exchange would cease unregistered crypto asset staking services and pay $30 million to settle the charges. On March 9th, New York Attorney General Letitia James filed a lawsuit against KuCoin, accusing it of failing to register as a securities and commodities broker-dealer while offering digital currencies such as ETH, which are classified as securities and commodities. This marks the first time regulators have claimed in court that ETH is a security. Ethereum is facing increasing regulatory pressure.

Although Ethereum still has many technical aspects to improve and multiple stages to complete on its roadmap, it remains the most powerful ecosystem, boasting the largest number of developers, funds, and users. Ethereum is expected to maintain its leading position in the Web3 space for the foreseeable future, driving innovation and development in the industry. Other public blockchains and Layer 2 solutions can leverage their strengths to become specialized application chains. The Web3 market is vast, and the future will be a multi-chain world.

Arbitrum Token Launch

On March 16th, the Arbitrum Foundation announced that it would airdrop its native token, ARB, to community members on March 23rd, sparking lively discussions in the crypto community.

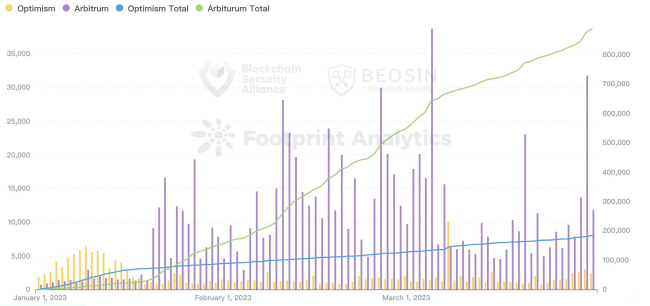
Arbitrum, as a leading Optimism Rollup, has strong fundamentals and has surpassed Optimism in protocol revenue during Q1, with an overall growing trend.



Arbitrum / Optimism / Ethereum Transactions Per Day

Arbitrum's daily transaction volume was previously on par with Optimism, but since mid-January, it has overtaken Optimism and expanded its leading advantage, reaching approximately 2-3 times that of Optimism. As of March 18th, Arbitrum's daily transaction volume was about 3.8 times that of Optimism. This is partly due to the contribution of top-tier protocols like GMX and popular games like Beacon within its ecosystem, and partly because of users' expectations for the airdrop.

The prosperity of the on-chain ecosystem largely depends on active developers driving it forward, and we can see that the number of contract deployments on Arbitrum in Q1 far exceeds that of Optimism.



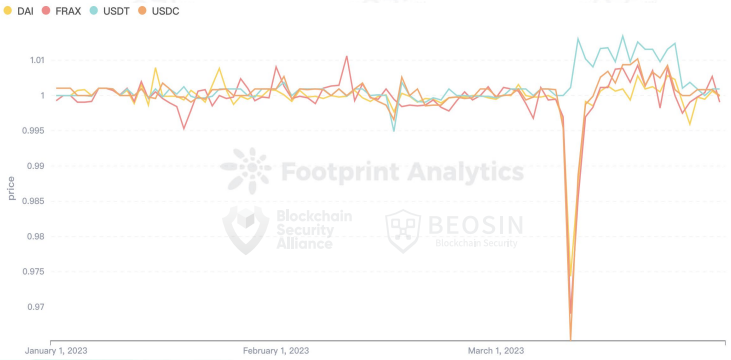
Daily L2 Contract Deployments

Token launches are not the end goal but rather the beginning of fostering a thriving ecosystem. Optimism took the initiative by using token incentives to activate its community, capturing 15% of the Layer 2 market share between October 2022 and January 2023. It is expected that Arbitrum will also implement measures to reward protocol users and stimulate ecosystem activity, expanding its influence in the Layer 2 space. Not only Optimism Rollup, but other Layer 2 solutions based on Zero Knowledge Rollup are also rapidly developing. The competition in Layer 2 is just beginning, and applications built on top of it will have the opportunity for rapid growth. Ethereum's moat will be further consolidated, so let's keep a close watch on these developments.

USDC Depeg

In recent years, stablecoins have developed rapidly, and regulators are increasingly concerned that the growth of stablecoins could affect the effectiveness of monetary policy decisions and pose systemic risks to traditional finance. On February 13th, the Wall Street Journal reported that the U.S. Securities and Exchange Commission (SEC) issued a Wells Notice to stablecoin issuer Paxos, intending to sue BUSD for being an unregistered security. On February 13th, Paxos announced it would stop minting BUSD, and Binance announced on March 17th that it had replaced its users' BUSD assets in the SAFU fund with TUSD and USDT. On March 9th, the U.S. Commodity Futures Trading Commission (CFTC) Chairman Rostin Behnam said that if Congress does not pass comprehensive digital asset regulations, stablecoins based on fiat currencies would be regulated as commodities. On March 13th, the International Monetary Fund warned G20 countries that widespread adoption of crypto assets could lead to banks losing deposits and reducing loans. Traditional finance professionals are concerned that the rise of stablecoins could impact the existing financial system. However, the dramatic collapse of Silicon Valley Bank has triggered a chain of events.

On March 10th, Silicon Valley Bank was ordered to close by the California Department of Financial Protection and Innovation due to its inability to handle a bank run and was taken over by the Federal Deposit Insurance Corporation (FDIC). Bloomberg reported that a regulatory filing indicated that 93% of Silicon Valley Bank's deposits were uninsured. On March 11th, Circle stated that $3.3 billion out of its $40 billion USDC reserves were held at Silicon Valley Bank. This news sparked market panic, leading to a sell-off of USDC, which at one point depegged to $0.9. Decentralized stablecoins DAI and FRAX, which are closely related to USDC, were also affected and briefly depegged. It was not until March 12th when U.S. Treasury Secretary Janet Yellen, Federal Reserve Chairman Jerome H. Powell, and FDIC Chairman Martin J. Gruenberg issued a joint statement announcing that depositors would be able to withdraw all cash starting from March 13th that market confidence gradually recovered, and the value of USDC gradually rebounded. As of March 18th, the proportions in Curve Finance's 3pool have not yet returned to their pre-incident equilibrium levels.



Stablecoin Price Q1 2023

Faced with the black swan event of USDC depegging, some projects holding USDC chose to take the loss and exchange it for USDT, some purchased ETH and BTC, while others chose to cash out to diversify risks. In the past, regulators believed that the traditional banking system needed protection from the impact of crypto assets, but this incident demonstrated that crypto entities need protection from the collapse of traditional banks. In light of the instability factors in the banking system, Binance even plans to convert its $1 billion BUSD industry recovery plan funds into native cryptocurrencies. This incident has also awakened some traditional finance professionals to the importance of self-custody of Bitcoin. On March 10th, the capital inflow into the ARK Innovation ETF, which holds a large position in Bitcoin-related assets, reached $397 million, setting a multi-year high. Bitcoin's price has since risen for several consecutive days.

The business logic of the banking system forces it to engage in maturity mismatches, making it prone to liquidity crises during interest rate hikes. This incident also exposed the overly concentrated and opaque flaws in the banking system, with bank deposits experiencing a year-on-year decline for the first time since the 1920s. Bitcoin, a decentralized, transparent, verifiable, and securely operated financial platform for many years, will gain more recognition in the future. As the title of the article cited in the first block of Bitcoin from The Times on January 3, 2009, stated, "Chancellor on brink of second bailout for banks," we need a better financial system.

Interestingly, the notoriously opaque USDT has gained more market share in this incident. However, to solve the centralized and opaque issues of crypto assets, stablecoins supported by native crypto assets are ultimately needed. AAVE is about to launch GHO, a stablecoin over-collateralized by a basket of cryptocurrencies, with interest rates determined by promoters and DAOs, unaffected by supply and demand. Curve plans to introduce crvUSD, a non-liquidatable over-collateralized stablecoin supported by LPs, further consolidating its leading position in the stablecoin exchange market. The stablecoin issuance platform Liquity is fully supported by algorithms and contracts, and the development team does not have the relevant permissions to modify the protocol, making it more censorship-resistant and decentralized. The battle of stablecoins continues, with multiple stablecoin projects likely to bundle and support each other, and develop collaboratively in the future.

IV.
Beosin Security Services and Products

Beosin Security Product

Beosin EagleEye

Security monitoring, alerting and blocking

Based on AI technology, combined with on-chain and off-chain real-time data analysis, and open source intelligence, it can timely discover security risks, send alerts and block risk transactions during the operation of Web 3.0 projects. Subscribers will receive real-time warnings for 10 kinds of abnormal risk transactions such as large transfers, flashloans, privilege changes, price drops, etc. It plays a role in hacking, fraud, rug pull and other security issues prevention. Now more than 2,300 Web 3.0 projects have been monitored by Beosin EagleEye.

Try Beosin EagleEye: https://eagleeye.beosin.com/

Add Beosin Alert to your browser to detect phishing sites:
https://chrome.google.com/webstore/detail/beosin-alert/lgbhcpagiobjacpmcgckfgodjeogceji?hl=en

Beosin KYT

AML and crypto compliance platform

Relying on more than 1 billion address tags and malicious address database, Beosin KYT, the cryptocurrency AML and crypto compliance platform can help VASP (Virtual Asset Service Providers) build KYT (Know Your Transactions) and risk assessment capabilities. The system analyzes massive amounts of on-chain transactions to identify transactions and address types, and then uses the system's massive library of entity addresses and machine learning analytics to assess risky transactions. Beosin KYT are currently serving multiple clients around the world to comply with AML regulations.

Try Beosin KYT: https://kyt.beosin.com/

Beosin Trace

Cryptocurrency tracing and investigation platform

Beosin-Trace is a cryptocurrency fund tracing platform that combines big data, AI and other technologies. It is a personalized investigation tool for global clients in recovering their lost cryptocurrencies. It has successfully helped clients recover 100+ millions of stolen assets, including funds that flowed into mixers (such as Tornado Cash).

Try Beosin Trace: https://beosin.com/service/tracing

Beosin VaaS

Formal verification platform for smart contracts

Beosin security team uses multiple technologies such as formal verification and fuzzy testing as core technologies to develop VaaS, a highly automated security detection tool for smart contracts, with an accuracy of 97% and can automatically detect hundreds of security vulnerabilities of smart contracts in one-click.

Try Beosin VaaS: https://vaas.beosin.com/

About Blockchain Security Alliance

Blockchain Security Alliance

The Blockchain Security Alliance was initiated by Beosin in joint collaboration with several units from diverse industry backgrounds, including university institutions, blockchain security companies, industry associations, fintech service providers, etc. The first batch of alliance council include Beosin, SUSS NiFT, NUS AIDF, BAS, FOMO Pay, Onchain Custodian, Semisand, Coinhako, ParityBit, and Huawei Cloud. The current members include: Huobi University, Moledao, Least Authority, PlanckX, Coding Girls, Coinlive, Footprint Analytics, Web3Drive, and Digital Treasures Center. The members of the Security Alliance will work and cooperate together to continuously secure the global blockchain ecosystem with their own technical strengths. The Alliance Council also welcomes more people in blockchain-related fields to join and jointly defend the security of the blockchain ecosystem.

Alliance Registration: https://forms.gle/pb3NaUgS3a2Sswnc8

Contact: @kristenbeosin @Web3Donny market@beosin.com

BEOSIN Blockchain Security

About Beosin

Beosin is a leading global blockchain security company co-founded by several professors from world-renowned universities and there are 40+ PhDs in the team. It has offices in Singapore, UAE, Korea, Japan and other 10+ countries. With the mission of "Securing Blockchain Ecosystem", Beosin provides "All-in-One" blockchain security solution covering Smart Contract Audit, Risk Monitoring & Alert, KYT/AML, and Crypto Tracing. Beosin has already audited more than 2500 smart contracts including famous Web3 projects PancakeSwap, Uniswap, DAI, OKSwap and all of them are monitored by Beosin EagleEye. The KYT AML are serving 100+ institutions including Binance.

LegalDAO

About LegalDAO

LegalDAO is a decentralized community that gathers global Web3 legal professionals and enthusiastic participants, dedicated to building a global Web3 legal ecosystem. Through initiating the bottom-up "2023 Crypto Consensus Referendum," establishing a social relationship-based on-chain identity system "De-X," a decentralized self-governance system "De-Reg," and Web3 legal research, education, socialization, and other content, we call on everyone to work together to complete the great practice of establishing Web3 native order.

SUSS NiFT Node for Inclusive Fintech

About SUSS NiFT

The SUSS Node for Inclusive Fintech (NiFT) is the "Centre of Excellence" spearheading all Fintech initiatives at the university. It is a multi-disciplinary centre drawing on expertise from faculty members across SUSS' five schools, their collective publications and programmes. Established in 2021, SUSS NiFT is essentially a re-launch of SUSS' endeavor in the Fintech and blockchain domain since 2016. NiFT serves to deliver high-quality research, public education, and policy advocacy for inclusivity in the Financial Technology sector for the benefit of society.

Footprint Analytics

About Footprint Analytics

Footprint Analytics is a data platform blending web2 and web3 data with abstractions. We help analysts, builders, and investors turn blockchain data into insights with accessible visualization tools and a powerful multi-chain API across 20+ chains for NFTs, GameFi and DeFi. We also provide Footprint Growth Analytics to help with effective growth in GameFi and any web3 projects.

CONTACT US

market@beosin.com
Email

@Beosin
Telegram

@Beosin_com
Official Twitter

@BeosinAlert
Alert Twitter